AO106 (Rev. 12/03) Affidavit for Search Warrant

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF ILLINOIS

In the Matter of the Search of
(Name, address or brief description of person, property or premises to be searched)
INFORMATION ASSOCIATED WITH Evernote account associated with Stephan4096@gmail.com THAT IS STORED AT PREMISES CONTROLLED BY Evernote Corporation.

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

Case Number: 18-MJ- 7130

I, TODD M. EMERY being duly sworn depose and say:

I am a(n) Special Agent for the Drug Enforcement Administration (Official Title) and have reason to believe

that ☐ on the person of or ☑ on the property or premises known as (name, description and/or location)
INFORMATION ASSOCIATED WITH Evernote account associated with Stephan4096@gmail.com THAT IS STORED AT PREMISES CONTROLLED BY Evernote Corporation, more particularly described in Attachment A, which is attached hereto and specifically incorporated herein.

in the Northern District of California

there is now concealed a certain person or property, namely (describe the person or property to be seized)
See Attachment B, which is attached hereto and specifically incorporated herein.

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)
fruits, contraband, evidence and instrumentalities.

concerning a violation of Title 21 United States code, Section(s) 841, 846

The facts to support a finding of probable cause are as follows:

See affidavit of Drug Enforcement Administration Special Agent Todd M. Emery, which is attached hereto and specifically incorporated herein.

Continued on the attached sheet and made a part hereof: ☑ Yes ☐ No

s/Todd M. Emery
Signature of Affiant

Sworn to before me and subscribed in my presence,

July 17, 2018 (Date) at Urbana (City) Illinois (State)

s/Eric I. Long

ERIC I. LONG (Name of Judge) Magistrate Judge (Title of Judge)

Signature of Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF ILLINOIS

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH **Evernote account associated with Stephan4096@gmail.com** THAT IS STORED AT PREMISES CONTROLLED BY **Evernote Corporation.**	18-mj-7130 Case No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Todd M. Emery being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Evernote Corporation, which is headquartered at 305 Walnut Street, Redwood City, California 94063. Evernote is a mobile application for note taking, organizing, tasks lists, and archiving, among other uses. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Evernote Corporation to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Drug Enforcement Administration and have been so employed for more than seven years. I have had extensive training in the investigation of drug related crimes and the enforcement of federal laws concerning controlled substances as found in Title 21 of the United States Code. Currently, I am assigned to the DEA's Springfield, Illinois, Resident Office (SRO). I have investigated illicit controlled substance trafficking, to include the importation, distribution, manufacture and cultivation of illegal substances. I have personally conducted or assisted in numerous investigations of state and federal criminal violations involving the illegal trafficking of narcotics and related crimes. I have received specialized training in various aspects of narcotics investigations, which includes but is not limited to interviewing defendants and witnesses, surveillance techniques, and money laundering. Prior to my assignment at SRO, I served as Technical Operations Agent to the DEA Imperial, California, District Office for approximately five years where I assisted agents in conducting cyber investigations, authored several search warrants to technical enterprises such as Microsoft and Facebook, and handled operations for that office's wire room to include assisting in routing data packets such as email content to approved systems for agent investigations. I also served two years at the DEA's Office of Special Intelligence, where I learned skillsets involving Virtual Private Networking (VPN), IP configuration, and basic programming in several computer coding languages. I have helped prepare numerous complaint and search warrant affidavits, participated in the execution of search warrants, and testified at criminal trials during my

participation in drug investigations.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 21 U.S.C. §§ 841(a)(1) and 846, Distribution of a Controlled Substance and Attempt to Distribute a Controlled Substance, have been committed by Stephan CAAMANO, of Champaign, Illinois, utilizing the Evernote account associated with the email address Stephan4096@gmail.com. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

Initiation of Investigation

6. In December 2017, agents began investigating a target, Stephan CAAMANO, for manufacturing controlled substance with tablet press machines

purchased online from various companies based in China. Customs and Border Protection agents had contacted the Drug Enforcement Administration's Springfield, Illinois, Resident Office pertaining to several imported items seized by CBP that were destined for delivery to CAAMANO.

7. CBP advised that on September 16, 2016, agents had seized a package from Mijdrecht, The Netherlands, that was inbound to CAAMANO at an address of 2562 Le Conte Avenue, Berkeley, California; the package contained 29 grams of 3,4-Methylenedioxymethamphetamine, or MDMA (commonly known as ecstasy). An open records search identified the address as student housing for the University of California-Berkeley; that residence was occupied by CAAMANO during his enrollment there.

8. CBP further advised that on April 18, 2017, agents had seized a package from Shanghai, China, that was inbound to CAAMANO at an address of 510 South Fair Street, Champaign, Illinois; the package contained one turbine wheel box pill press machine. The agents' investigation has not revealed any renter other than CAAMANO at the time of the seizure.

9. CBP advised that on June 13, 2017, agents had seized a package from an unknown shipper that was inbound to CAAMANO at an address of 1717 West Kirby Avenue, #108, Champaign, Illinois; the package contained 109 grams of Fentanyl and 210 grams of Alprazolam (Xanax). That address corresponds to a mailing box at a UPS store; agents have confirmed that CAAMANO rents that box.

10. CBP advised on July 13, 2017, agents had seized seven packages from Shanghai, China, that were inbound to CAAMANO at an address of 202 South Broadway Avenue, #142, Urbana, Illinois; these packages contained drilling machine bolts for a tablet press machine. Agents have confirmed through United States Postal Investigation Services that CAAMANO had rented Post Office Box 142 at this location, the Urbana Post Office, during the time of the seizure.

11. I also obtained a copy of a University of Illinois Urbana-Champaign Police Department (UIUC PD) report taken on October 25, 2016, where a campus housing maintenance worker completing a work order request observed what was believed to be drug related equipment at 2101 Hazelwood Ct., Apt 204, Urbana, Illinois. The Police Department responded and spoke with the resident, CAAMANO, concerning the equipment. CAAMANO advised the chemicals, pills, and tablet press machine were for health supplement pills that he wanted to manufacture.

Surveillance of CAAMANO and Package Drop

12. On March 8, 2018, agents conducted surveillance of CAAMANO at his residence, 1510 Glenshire Drive, Champaign, Illinois.[1] At approximately 10:00 a.m., agents observed CAAMANO depart his residence traveling eastbound on Kirby

[1] Agents previously had performed an open source records search and learned utilities in Stephan CAAMANO's name had been established at 1510 Glenshire Drive, Champaign, Illinois. Agents also had discovered via subpoenaed bank records that CAAMANO had purchased the property in full with a wire transaction to the seller's bank under the business name Longevity Realty Management LLC.

Avenue in a 2017 Toyota RAV4, blue in color, bearing Illinois License Plate AM93634, and assigned vehicle identification number 2T3BFREV5HW647548. That vehicle is registered to and known to be driven by CAAMANO. Agents observed CAAMANO arrive in the RAV4 at a United States Postal Service drop box located near 2012 Round Barn Road, Champaign, Illinois. Agents then observed and video recorded CAAMANO as he removed yellow manila envelopes from the rear passenger area of his vehicle multiple times and deposited said manila envelopes into the USPS drop box.

13. That same morning, while maintaining surveillance of the drop box, agents contacted the United States Postal Inspection Service so that they could visually inspect the manila envelopes deposited in the USPS drop box by CAAMANO. USPIS sent a mail carrier to open the drop box near 2012 Round Barn Road, Champaign, Illinois, and to collect all mail from inside the drop box.

14. Later that morning, at approximately 11:15 a.m., agents met with the USPS mail carrier at the Round Barn Road location. Prior to the mail carrier's arrival, agents confirmed via surveillance that no other individuals had gained access to the USPS drop box or tampered with its contents. With assistance from the USPS mail carrier, agents were able to visually inspect the contents of the drop box and observed 33 yellow manila envelopes matching in appearance the yellow manila envelopes agents previously saw CAAMANO depositing into the drop box. No other item in the drop box outside those 33 envelopes was comparable to the items agents observed and video recorded CAAMANO depositing in the drop box.

15. Also on March 8, 2018, at approximately 2:00 p.m., agents traveled to the United States Post Office, located at 600 North Neil Street, Champaign, Illinois, where the USPS mail carrier who assisted at the USPS drop box near 2012 Round Barn Road, Champaign, Illinois, had directly taken the 33 manila envelopes identified as matching the manila envelopes deposited by CAAMANO.

16. Agents visually inspected each of the 33 manila envelopes and observed that the return sender on each of the 33 envelopes was listed as a "Colin H. Taylor". Agents also observed a shipping company, EasyPost, had created the shipping label on each envelope, and all envelopes had the same EasyPost account number: C26321.

17. Agents interviewed the USPS mail carrier who advised similar manila envelopes had been deposited into four USPS drop boxes in the vicinity of Mattis Avenue and Kirby Avenue in Champaign, Illinois, each day for more than a year. The mail carrier estimated the number of manila envelopes to be between 50 and 100 among the four drop boxes each day.

18. The USPS mail carrier stated he made a formal complaint in March 2017 to management about the quantity of manila envelopes, which had been making his collection duties very difficult to complete. The mail carrier advised that at the time of the complaint his management contacted the shipper, identified as "Sharon Lee", and advised a non-fictitious mailing address was required, otherwise the manila envelopes would not be shipped. The mail carrier provided a photograph to agents of a manila envelope seen in March 2017 bearing the return shipping name "Sharon Lee". Agents

observed the shipping label was created by EasyPost and was associated with the same account number: C26321.

Recovery of Alprazolam in Champaign County

19. On March 9, 2018, agents received information from the Champaign County Sheriff's Office concerning an incident report involving recovered property. On February 21, 2018, the Sheriff's Office took a report at 3206 Halifax Drive, Apartment B, Champaign, Illinois, in which a female subject, identified as T.A., received four boxes delivered to her by USPS, each identifying her as the "return sender". T.A. told the Sheriff's Office that she did not send any boxes and opened one to check its contents. Upon inspection, T.A. observed three gray packages, wrapped in bubble wrap, inside the box. T.A. then opened one gray package and discovered numerous pills, all marked with "Xanax" on each pill. T.A. relinquished custody of the four boxes and their contents to the Sheriff's Office.

20. Agents reviewed photographs taken of the shipping labels on the four boxes and observed a shipping label created by EasyPost with the same account number as the one used on envelopes bearing the return address names "Colin H. Taylor" and "Sharon Lee". The EasyPost account number was C26321.

21. On March 12, 2018, agents took custody of the four boxes and their contents from the Sheriff's Office. Agents inspected the contents and confirmed the four boxes were each filled with three packages. Each of the three packages contained numerous white elongated pills. Agents observed that each pill bore the marking

"Xanax" on one side and the marking "2" on the other side, which markings are consistent with pills made by the pharmaceutical manufacturer Pfizer. Agents could tell upon inspecting the pills through the plastic packaging that several of the pills had lighter markings, indicating possible counterfeit production. On March 27, 2018, laboratory results returned indicating the pills were all alprazolam (Xanax) with a 95% level of confidence and numbered 83,538 dosage units (total pills).

Cleveland Alprazolam Package

22. Meanwhile, on March 8, 2018, Cleveland Police Department Detective John Dlugalinski reported USPS Parcel 9405536897846313514706 (Easy Post) to United States Postal Inspection Services Investigator Bryon Green. The parcel was addressed to 3740 Euclid Ave, Cleveland, Ohio, 44115, and was turned over by a resident who had no knowledge of the parcel. The parcel originated in Urbana, Illinois. The parcel contained more than 1,000 alprazolam pills; the presence of alprazolam was confirmed by the Cuyahoga County Laboratory on March 22, 2018.

23. On March 22, 2018, Investigator Green identified associated mailings going to Nicholas Armstrong[2] at 1443 E. 25th St. in Cleveland, Ohio 44114. These parcels, like those deposited by CAAMANO into the mail drop box in Champaign,

[2] Armstrong was a co-defendant with Nick J. Powell in Cuyahoga County Case #CR-15-593701-B. Powell currently resides in Florida and is under investigation by New York USPIS Investigator Michael Slavkovsky and others in relation to alprazolam sales on the darkweb.

Illinois, had a return address of Colin H. Taylor, 2105 S. Zuppke Dr., Urbana, Illinois, and were associated with EasyPost account C26321.

24. On March 26, 2018, Investigator Green, along with Homeland Security Investigations and the Drug Enforcement Administration, conducted a controlled delivery of the parcels destined for Armstrong. Agents detained Armstrong after he took custody of the parcels and returned to his residence. Armstrong signed a consent form permitting law enforcement agents to search his residence, which resulted in the recovery of the two parcels associated with EasyPost account C26321, along with various narcotics, numerous Priority Mailing envelopes, label makers, and a food saver machine with plastic bags commonly used for vacuum packaging.

25. Armstrong provided a statement to agents and advised he purchased the "Xanax" (alprazolam) that was recovered from the parcels from a darkweb vendor that Armstrong had found on a Reddit forum. He identified the Reddit user as "Googleplex". Armstrong stated that "Googleplex" sells "Xanax" on the Dream Market, but advised that he purchased directly from "Googleplex" by sending Monero[3] cryptocurrency to a wallet[4] provided by "Googleplex". Armstrong stated he

---

[3] An open-source cryptocurrency that focuses on privacy and decentralization. Monero uses a public ledger to record transactions while new units are created through a process called mining. Monero aims to improve on existing cryptocurrency design by obscuring sender, recipient, and amount of every transaction made, as well as making the mining process more egalitarian.

[4] A "wallet" or cryptocurrency wallet stores the public and private keys, which can be used to receive or spend the cryptocurrency. A wallet can contain multiple public and private

communicates with "Googleplex" via email. Armstrong stated he ordered from "Googleplex" three times in amounts of $5,000.00, $5,000.00, and $4,000.00 and paid "Googleplex" $0.60 per "Xanax" pill.

26. In performing a Google search using keywords "Googleplex Reddit", agents were able to see URL results ranging from 2016 to 2018, which referenced "Googleplex" and discussed dark web transactions and "Xanax".

PayPal Purchases

27. On December 19, 2017, and March 1, 2018, I issued administrative subpoenas to PayPal for information regarding purchases funded by Navy Federal Credit Union checking account 7029731721 belonging to CAAMANO. These purchases were made via PayPal accounts that were registered using the Google, Inc. email accounts stephancho@gmail.com, Stephan4096@gmail.com, Mexacc702x@gmail.com, and torimoneybags@gmail.com.

a. Email account stephancho@gmail.com was registered to PayPal account 1662394575525739130 that was used to purchase Firmapress, a pharmaceutical binding agent, from the company LFA Machines Oxford Ltd on April 4, 2017.

---

key pairs. The cryptocurrency itself is not in the wallet. The cryptocurrency is decentrally stored and maintained in a publically available ledger. With a private key, it is possible to write in the public ledger in order to spend the cryptocurrency.

b. Email accounts stephancho@gmail.com and stephan4096@gmail.com were registered to PayPal account 1928865671187482181 used to purchase Firmapress, a pharmaceutical binding agent, from company LFA Machines Oxford Ltd on September 19, 2016; December 14, 2016; December 19, 2016; March 6, 2017; April 19, 2017; May 19, 2017; June 25, 2017; July 12, 2017; September 4, 2017; and September 29, 2017. This same account was used to purchase from LFA Machines Oxford Ltd a RTP 9 Rotary Tablet Press on April 26, 2017 and a Tablet Dust Vacuum on August 8, 2017. This account also was used to purchase additional tablet press machines from vendor eb@senders-inc.com on December 14, 2016, and vendor cabbo@live.cn on December 22, 2016; binding and tablet machine parts from vendor petter.su@outlook.com on February 6, 2017, and March 26, 2017; and oval and polygon punch stamp molds for tablet press machines from vendor weiping002@hotmail.com on December 21, 2016.

c. Email account Mexacc702x@gmail.com was registered to PayPal account 2073608850950743797 used to purchase a 20-liter Mixer Pharma machine and rotary press machine from vendor Capsulcn International Company Ltd on March 12, 2017, and March 28, 2017.

d. Email account torimoneybags@gmail.com was registered to PayPal account 2207517011988366384 used to purchase a 20-liter Mixer Pharma

machine from vendor Capsulcn International Company Ltd on August 18, 2016; a single punch tablet press machine from vendor Xie Dian Mou on September 6, 2016; a Xanax punching mold die set stamping mold for a tablet press machine from vendor 侯 茜桐 on October 6, 2016; and polygon die stamp molds for a tablet press machine from vendor Ping Wei on October 6, 2016.

Trash Pulls and Additional Surveillance

28. Throughout the course of this investigation, law enforcement agents have conducted a series of trash pulls at 1510 Glenshire Dr. and at Stephan CAAMANO's rental address: 510 S. Fair Street, Champaign, Illinois, 61821.

29. Trash pulls on the following dates at 1510 Glenshire Dr. have revealed items including but not limited to:

a. **January 24, 2018**: Shipping labels addressed to CAAMANO at 1510 Glenshire Dr. and a known prior residence from Provident Machine Bearings, a precious metals dealer, and NutraHealthSupply.com, a nutrition bodybuilding supplement provider); numerous shredded plastic pieces with some sort of residue from what appeared to be several commercial grade plastic Ziploc bags; and a Netgear router instruction manual.

b. **January 31, 2018**: (1) A Budget rental agreement, showing that on August 27, 2017, CAAMANO rented a 26-foot diesel cargo trailer to move

property from 510 S. Fair Street, Champaign, Illinois, to 1510 Glenshire Dr.. (2) A shipping label addressed to Stephen CAAMANO at 1510 Glenshire Dr. The sender on the shipping label was Choetech, a company based in Lexington, Kentucky. Agents' research has revealed that the company is a supplier of electronic and computer accessory items, such as charging cords and USB connecting cables.

c. **April 11, 2018**: Numerous items including utility bills for 510 S. Fair Street, tax forms associated with CAAMANO, documentation of Post Office Box openings and closings, and a Navy Federal Credit Union mailing to CAAMANO. Agents also discovered a Christmas card to CAAMANO from Veldt Gold, a company known to sell precious metals in exchange for virtual currency.

d. **April 25, 2018**: Two Amazon shipping labels addressed to Eli LEE at 1510 Glenshire Drive.

e. **May 23, 2018**: Assorted shipping materials, including mylar packaging, vacuum sealer roll packaging, and unused shipping labels; assorted packaging envelopes addressed to CAAMANO at 1510 Glenshire Dr., 510 South Fair Street, and 302 East Green Street, Unit 2394, in Champaign, Illinois; a used Ziploc bag with powdery residue; industrial plastic bag with "DNP 200mg" written in marker; and a Provident Metals magnet (the precious metals dealer mentioned previously).

30. Trash pulls on the following dates at 510 S. Fair Street, Champaign, Illinois, 61821, have revealed items including but not limited to:

a. **March 27, 2018**: Two shipping documents addressed to CAAMANO at 510 S. Fair Street; three glass beakers; a charging device; a plastic bag with a white powdery residue; two plastic cups with white powdery residue; and six unopened packages of powder supplements.

b. **May 8, 2018**: 18 metal container rings and clamps, along with 15 metal lids. Many of the lids contained a powdery residue. All shipping labels on the metal lids had been forcibly removed, preventing agents from learning the shipper or container contents. Agents believe the clamps and lids were part of the packaging used to ship Firmapress, a pill binding agent, from LFA Machines, LLC.

Residential Search Warrants at Glenshire and Fair Residences

31. On May 27, 2018, residential search warrants were executed at 1510 Glenshire Drive and 510 South Fair Street in Champaign, Illinois. Stephan CAAMANO's rental residence, 510 South Fair Street, was largely empty, although law enforcement agents found various metal machine parts, proof of residency, an instruction manual for a scale, a Toshiba laptop, and a cutting agent powder.

32. At the 1510 Glenshire Drive address, agents found one zp9 rotary tablet press, two 20L mixing machines, 3 commercial grade scales, 3 heavy duty vacuum sealing machines, multiple large plastic bins and containers used to sort and mix

powders used to press pills, a container filled with binding agent Firmapress, pressed counterfeit Xanax bars, non-prescribed steroids, doping masking agents, non-FDA approved tramadol and domperidone medicines, tryptamine (psychedelic), multiple materials used for packaging and shipping items via registered mail, multiple cellular devices, and several computers and computer related components containing memory/hard drive space. The pill press had been partially taken apart. Agents also discovered a laptop cord to a Toshiba laptop. Agents did not encounter all of the pill presses CAAMANO appeared to have purchased via PayPal. Additionally, agents located empty shipping packages addressed to Eli LEE at 1510 Glenshire Dr. and a bill addressed to Eli LEE.

Evernote Account

33. Information was obtained from a cellular device, taken at the time of CAAMANO's arrest, which showed numerous accounts activated on the device. One of those accounts was listed as **Evernote** and associated to Google account Stephan4096@gmail.com, one of the email accounts associated with a PayPal account used to purchase pill presses and other materials. Also found on the cellular device was evidence of cryptocurrency and TOR applications, which suggested the device had been set up to assist CAAMANO with dark web activities.

34. On May 29, 2018, agents sent a preservation request to Evernote pertaining to all records associated under email account Stephan4096@gmail.com. In general, electronic data sent to an Evernote subscriber is stored in the subscriber's

account information or Evernote forums on Evernote servers until the subscriber deletes the electronic data. If the subscriber does not delete the data, the data can remain on Evernote Corporation servers indefinitely. Even if the subscriber deletes the data, it may continue to be available on Evernote's servers for a certain period of time.

ADDITIONAL BACKGROUND REGARDING EVERNOTE

35. In my training and experience, I have learned that Evernote Corporation provides an on-line service to the public to take notes, organize, create task lists, and archive data, including but not limited to email messages. Evernote Corporation allows subscribers to use Evernote by linking it to a Google, Inc. email account or to another other email service. During the registration process, Evernote Corporation asks subscribers to provide basic personal information. Therefore, the computers of Evernote Corporation are likely to contain stored electronic communications and information concerning Evernote Corporation services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

36. An Evernote Corporation subscriber also can store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), documents, and other files, on servers maintained and/or owned by Evernote Corporation. These other services, files and/or

information may include: voice number; customer phone number; customer name and date of birth; other email address; names – including subscriber names, user names, and screen names; addresses - including payment addresses, mailing addresses, residential addresses, business addresses, and email addresses; local and long distance telephone records; telephone or instrument numbers (including MAC addresses, ESNs, MEINs, MEIDs, MINs, SIMs, MSISDNs, IMSIs, or IMEIs); and other subscriber numbers or identities, including the IP address and Port number. These records may also include purchase and sales records, virtual currency transactions, other financial records and information. In my training and experience, evidence of who was using an account may be found in address books, contact or buddy lists, email or other messages in the account, attachments to emails, including pictures and files, and other records and information saved in the account.

37. In my training and experience, application providers generally ask their subscribers to provide certain personal identifying information when registering for an electronic storage account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know

that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

38. In my training and experience, application providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, application providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

39. In my training and experience, in some cases, application account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Application providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes

under investigation because the information can be used to identify the account's user or users.

40. In my training and experience, individuals use applications like Evernote to save important data, communications and records, which may include evidence of criminal activity, including but not limited to email and other messages, purchase and sales transactions, financial data and accounts, and passwords to dark web sites and accounts.

41. This application seeks a warrant to search all responsive records and information under the control of Evernote Corporation, a provider subject to the jurisdiction of this court, regardless of where Evernote Corporation has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Evernote Corporation's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.[5]

---

[5] It is possible that Evernote Corporation stores some portion of the information sought outside of the United States. In *Microsoft Corp. v. United States*, 2016 WL 3770056 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, I respectfully request that this warrant apply to all responsive information—including data stored outside the United States—pertaining to the identified account that is in the possession,

42. As explained herein, information stored in connection with an application account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an application account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the application provider can show how and when the account was accessed or used. For example, as described below, application providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the application account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further

---

custody, or control of Evernote Corporation. The government also seeks the disclosure of the physical location or locations where the information is stored.

indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the application account owner's state of mind as it relates to the offense under investigation. For example, information in the application account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

43. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Evernote Corporation, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

s/Todd M. Emery

Todd M. Emery
Special Agent
Drug Enforcement Administration

Subscribed and sworn to before me on 7/17, 2018

s/Eric I. Long

The Honorable Eric I. Long
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Evernote account associated to email stephan4096@gmail.com, that is stored at premises owned, maintained, controlled, or operated by Evernote Corporation, a company headquartered at 305 Walnut Street, Redwood City, California, 94063.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Evernote Corporation (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on date April 5, 2018, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

(a) The contents of all emails or other communications associated with the account, including stored or preserved copies of communications, draft messages, the source and destination addresses associated with each message, the date and time at which each message was sent, drafted or saved, and the size and length of each message;

(b) All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers; records of session times and durations; the date on which the account was created; the length of service; the IP address used to register the account; log-in IP addresses associated with session times and dates; account status; alternative email addresses provided during registration; methods of connecting; log files; and means and source of payment (including any credit or bank account number);

(c) The types of service utilized to include, but not limited to the following:

i. Voice Number

ii. Customer Phone Number

iii. Customer Name and Date of Birth

iv. Other Email Address

(d) Names – including subscriber names, user names, and screen names;

(e) Addresses - including payment addresses, mailing addresses, residential addresses, business addresses, and email addresses;

(f) Local and long distance telephone records

(g) Telephone or instrument numbers (including MAC addresses, ESNs, MEINs, MEIDs, MINs, SIMs, MSISDNs, IMSIs, or IMEIs;

(h) Other subscriber numbers or identities, including the IP address and Port number;

(i) All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, financial data, purchase and sales records, and other files;

(j) All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

(k) For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 21 U.S.C. §§ 841(a) and 846, those violations involving Stephan CAAMANO (Evernote account associated with stephan4096@gmail.com) and occurring after January 1, 2016, through the present, including, for each account or identifier listed in Attachment A, information pertaining to the following matters:

(a) Any and all documents, records or information[1] relating to the purchase, sale, importation, possession, shipment, tracking, delivery or distribution of controlled substances, to include information regarding dark web or dark web marketplaces; conversations about Xanax, narcotics, drugs, or any pharmaceutical pills or materials; and "preparatory steps taken in furtherance of the scheme;

(b) Any and all documents, records or information relating to the purchase, sale, importation, possession, shipment, tracking, delivery or distribution of packaging materials;

(c) Any and all documents, records or information relating to the purchase, sale, tracking, delivery or distribution of postage or express mail consignment;

(d) Any and all documents, records or information relating to the transfer, purchase, sale or disposition of virtual currency;

(e) Any and all documents, records or information relating to the transfer, purchase, sale or disposition of precious metals;

(f) Any and all documents, records or information relating to the operation of money transmitting businesses;

(g) Any and all documents, records, or information relating to the access, creation and maintenance of websites and hidden (Tor-based) services;

(h) Any and all documents, records, or information relating to email accounts used in furtherance of these offenses;

---

[1] As used above and on, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage.

(i) Any and all records or other items which are evidence of ownership or use of computer or other electronic equipment, including, but not limited to, sales receipts, bills for internet access, and digital manuals.

(j) Any and all records relating to an indicia of occupancy, residency, and ownership or use of rental or purchased properties, including, but not limited to, utility and telephone bills; rental, purchase or lease agreements; and identification documents;

(k) Any and all records of any address and/or telephone books, and any records or electronic data reflecting names; addresses; telephone numbers; pager numbers of co-conspirators; sources of controlled substances, precious metals and/or virtual currency; identifying information for customers purchasing controlled substances; and/or virtual currency;

(l) Any and all bank records, checks, credit card bills, account information, safe deposit box information and other financial records;

(m) Any and all copies of income tax returns filed with the Internal Revenue Service (IRS) or the Illinois Department of Revenue;

(n) Evidence of who used, owned, or controlled the account at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, access history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

(o) Evidence of the times the account was accessed;

(p) Passwords, encryption keys, and other access devices;

(q) Contextual information necessary to understand the evidence described in this attachment;

(r) Evidence of internet activity, including screenshots or other downloads from the Internet;

(s) Any and all records and information regarding hidden services accounts[2]

---

[2] Hidden services (.onion services) are accessed through the Tor anonymity network. Most are considered dark web services with no legitimate or identified service provider to which legal process may be served.

used in furtherance of the offenses described above, including, but not limited to, darknet market accounts, associated darknet forum accounts and Tor-based email accounts.

(t) Any and all records and information regarding peer to peer (P2P) virtual currency trading platform accounts, including, but not limited to, localbitcoins.com[3] accounts or bitcon-otc internet relay chat channel[4] accounts.

(u) Any and all records and information regarding virtual currency in any format, including but not limited to, wallets (digital and paper), public keys (addresses) and private keys.

(v) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

(w)Evidence indicating the account owner's state of mind as it relates to the crime under investigation;

(x) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

---

[3] LocalBitcoins, OY (and their associated web platform, localbitcoins.com "LBC") is a Finnish company which is not a licensed money transmitting business registered with the U.S. Government and compliant with the Bank Secrecy Act, which requires establishment and maintenance of anti-money laundering (AML) programs in accordance with know your customer (KYC) rules, such as identifying persons involved in currency transactions over certain thresholds. LBC is not considered a legitimate service provider to which legal process may be served for accurate subscriber information or account seizure.

[4] Internet Relay Chat (IRC) is a decentralized chat system which enables people with an installed client (computer program which sends and receives messages to and from an IRC server via the internet) to join in live discussions with anyone else connected in the same manner. The IRC server ensures that all messages are broadcast to everyone participating in a discussion. There can be many discussions going on at once; each one is assigned a unique channel. One such channel is #bitcoin-otc, in which virtual currency trades are negotiated and arranged. All transactions that may occur are conducted directly between counterparties, without any participation or intermediation from the hosts of IRC servers, and therefore no entity to which legal process may be served for accurate subscriber information, transactional history or account seizure.

(y) The identity of the person(s) who communicated with the user ID about matters relating to manufacturing and distributing counterfeit pharmaceuticals/narcotics, including records that help reveal their whereabouts.